Content Protection for Recordable Media Specification

DVD Book

Intel Corporation
International Business Machines Corporation
Matsushita Electric Industrial Co., Ltd.
Toshiba Corporation

Revision 0.96
January 31, 2003

This page is intentionally left blank.

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. IBM, Intel, MEI, and Toshiba disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

This document is an intermediate draft and is subject to change without notice. Adopters and other users of this specification are cautioned that products based on it may not be interoperable with the final version or subsequent versions thereof.

Intellectual Property

Implementation of this specification requires a license from the 4C Entity, LLC.

Contact Information

Please address inquiries, feedback, and licensing requests to the 4C Entity, LLC:

- Licensing inquiries and requests should be addressed to cprm-licensing@4Centity.com.
- Feedback on this specification should be addressed to cprm-comment@4Centity.com.

The URL for the 4C Entity, LLC web site is http://www.4Centity.com.

This page is intentionally left blank.

Table of Contents

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

1.

1.1 Purpose and Scope

The *Content Protection for Recordable Media Specification* defines a robust and renewable method for protecting content stored on a number of physical media types. The specification is organized into several "books". The *Introduction and Common Cryptographic Elements* book provides a brief overview of Content Protection for Recordable Media (CPRM), and defines cryptographic procedures that are common among its different uses. This document, the *DVD Book*, specifies additional details for using CPRM technology to protect content stored on recordable DVD media.

The use of this specification and access to the intellectual property and cryptographic materials required to implement it will be the subject of a license. A license authority referred to as the 4C Entity, LLC is responsible for establishing and administering the content protection system based in part on this specification. Note that this document describes the use of CPRM for several DVD formats, each of which may represent a separate license category with separate associated fees, as indicated by the CPRM license agreement.

1.2 Document Organization

This document is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 describes device requirements related to CPRM for recordable DVD media.
- Chapter 3 describes the location and format of common CPRM components on DVD-RAM media.
- Chapter 4 describes the location and format of common CPRM components on DVD-R and DVD-RW media.
- Chapter 5 describes the use of CPRM to protect Video Recording formatted content.
- Chapter 6 defines mechanisms used to implement CPRM for recordable DVD media in a PC based system.

1.3 References

This document shall be used in conjunction with the following publications. When the publications are superceded by an approved revision, the revision shall apply.

4C Entity, LLC, *CPRM license agreement*

4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 0.94*

4C Entity, LLC, *CSS-based DVD Drive Authentication for CPRM, Revision 0.9*

4C Entity, LLC, *Content Protection System Architecture White Paper, Version 0.81*

DVD Forum, *DVD Specifications for Rewritable Disc, Part 1: Physical Specifications, Version 2.1*

DVD Forum, *DVD Specifications for Rewritable Disc, Part 2: File System Specifications, Version 2.0*

DVD Forum, *DVD Specifications for Recordable Disc for General, Part 1: Physical Specifications, Version 2.0*

DVD Forum, *DVD Specifications for Recordable Disc for General, Part 1: Physical Specifications, Version 2.0 Supplemental Information*

DVD Forum, *DVD Specifications for Recordable Disc for General, Part 2: File System Specifications, Version 2.0*

DVD Forum, *DVD Specifications for Re-recordable Disc, Part 1: Physical Specifications, Version 1.1*

DVD Forum, *DVD Specifications for Re-recordable Disc, Part 2: File System Specifications, Version 1.0*

DVD Forum, *DVD Specifications for DVD-RAM/DVD-RW/DVD-R for General Discs, Part 3: Video Recording Specifications, Version 1.1*

DVD Forum, *DVD Specifications for DVD-RAM/DVD-RW/DVD-R for General Discs, Part 3: Video Recording Specifications, Version 1.1 Supplemental Information*

Mt. Fuji Commands for Multimedia Devices Version 5 Revision 1.00

1.4 Future Directions

This document currently provides details specific to using CPRM for the Video Recording format on DVD-RAM media, DVD-R media and DVD-RW media. It is anticipated that CPRM technology will also be applied to other DVD formats, e.g. Stream Recording format and Audio Recording format, under future extensions to this specification, as authorized by the 4C Entity, LLC.

1.5 Notation

Except where specifically noted otherwise, this document uses the same notations and conventions for numerical values, operations, and bit/byte ordering as described in the *Introduction and Common Cryptographic Elements* book of this specification.

1.6 Abbreviations and Acronyms

The following is an alphabetical list of abbreviations and acronyms used in this document:

4C	4 Companies (IBM, Intel, MEI, and Toshiba)
ACC	Authentication Control Code
AGID	Authentication Grant ID
APSTB	Analog Protection System Trigger Bits
AV	Audio-Visual
ASCII	American Standard Code for Information Interchange
Auth	Authentication
BCA	Burst Cutting Area
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CGMS	Copy Generation Management System
CPRM	Content Protection for Recordable Media
CPR_MAI	Copyright Management Information
CSS	Content Scramble System
DCI_CCI	Display Control Information and Copy Control Information

DVD	Digital Versatile Disc
DVD-R	Digital Versatile Disc – Recordable
DVD-RAM	Digital Versatile Disc – Rewritable
DVD-ROM	Digital Versatile Disc – Read-only Memory
DVD-RW	Digital Versatile Disc – Re-recordable
ECB	Electronic Codebook
ECC	Error Correction Code
EPN	Encryption Plus Non-assertion
ID	Identifier
LLC	Limited Liability Company
lsb	Least Significant Bit
MAC	Message Authentication Code
MKB	Media Key Block
MPEG	Moving Picture Experts Group
msb	Most Significant Bit
NBCA	Narrow Burst Cutting Area
PC	Personal Computer
PES	Packetized Elementary Stream
RDI	Real-time Data Information
VMGI_MAT	Video Manager Information Management Table

This page is intentionally left blank.

Chapter 2
Device Requirements

2.

2.1 Device Keys

For the first generation, each CPRM compliant DVD Recording or Playback Device is given a set of 16 secret Device Keys, denoted K_{d_0},K_{d_1},...,K_{d_15}. These keys are provided by the 4C Entity, LLC, and are for use in processing the MKB to calculate the Media Key (K_m), as described in the *Introduction and Common Cryptographic Elements* book of this specification. Key sets may either be unique per device, or used commonly by multiple devices. The CPRM license agreement describes the details and requirements associated with these two alternatives. A device shall treat its Device Keys as highly confidential, and the associated Row values as confidential, as defined in the CPRM license agreement.

This page is intentionally left blank.

Chapter 3
CPRM Components on DVD-RAM Media

3. Introduction

This chapter specifies the location and format details of the common CPRM components described in the *Introduction and Common Cryptographic Elements* book of this specification, when stored on DVD-RAM media. The DVD-RAM format is the subject of a license from the DVD Forum, which also publishes specifications describing the format in detail (see the corresponding references in Section 1.3):

- DVD Specifications for Rewritable Disc, Part 1: Physical Specifications
- DVD Specifications for Rewritable Disc, Part 2: File System Specifications

This chapter assumes the reader is familiar with the DVD-RAM format, and focuses on those aspects of the format that are relevant to CPRM protection. Figure 3-1 gives an overview of the locations of CPRM related components on DVD-RAM media.

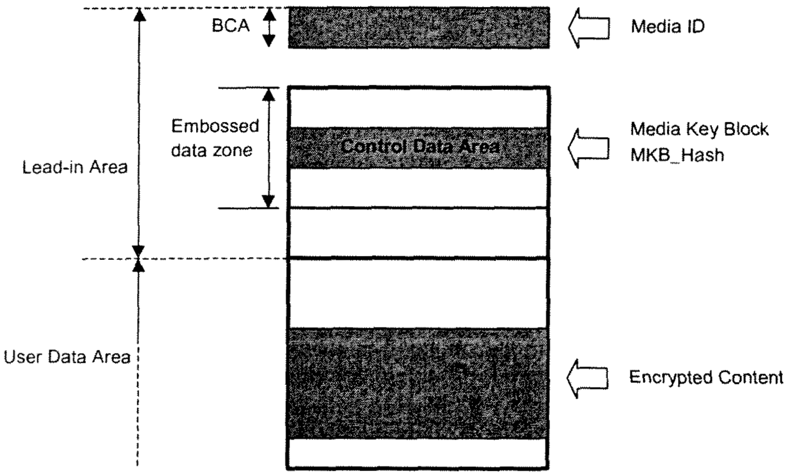


Figure 3-1 – Physical Layout of Common CPRM Components on DVD-RAM Media

- A Media Identifier (ID_{media}) is pre-recorded in the Burst Cutting Area (BCA).
- A Media Key Block (MKB) is pre-recorded in the Embossed data zone of the Lead-in Area.
- An MKB_Hash is pre-recorded in the Embossed data zone of the Lead-in Area.
- Encrypted Content is recorded in the User Data Area.

In addition, other application-specific components related to CPRM may also be stored in the User Data Area, as described later in the chapters of this document covering application formats.

The remainder of this chapter contains further details on the location and format of the Media Identifier and MKB. DVD-RAM media containing a Media Identifier and MKB as described in this chapter will be referred to as CPRM compliant DVD-RAM media.

3.1 Media Identifier

CPRM compliant DVD-RAM media shall contain a 64-bit Media Identifier (ID_{media}), which is placed in the Burst Cutting Area (BCA) by the media manufacturer. The BCA can contain multiple, contiguous blocks of data, called BCA Records, each containing information for a different use. Each BCA Record begins with a 2-byte BCA Record ID field identifying the Record's use, followed by a 1-byte Version Number field, followed by a 1-byte Data Length field indicating the length, in bytes, of the remaining data in the Record. Devices must not assume a fixed location or size for a given BCA Record, and must instead use the BCA Record ID and Data Length fields to go from one Record to the next until the desired Record is found. For CPRM compliant DVD-RAM media, the BCA shall include a BCA Record containing the Media Identifier, with format as shown in Table 3-1.

Table 3-1 – Format of BCA Record Containing the Media Identifier

Bit Byte	7	6	5	4	3	2	1	0
0	(msb)			BCA Record ID: 0002_{16}				
1								(lsb)
2				Version Number: 01_{16}				
3				Data Length: 08_{16}				
4	(msb)			Record Data: Media Identifier				
:								
11								(lsb)

The BCA Record ID field identifies the use for the BCA Record, with the value 0002_{16} indicating a Media Identifier Record. For the Media Identifier Record, the Version Number field is currently defined as 01_{16}. The Data Length field indicates the length in bytes of the subsequent Record Data field, which is 08_{16} for the Media Identifier Version 01_{16}. The Media Identifier itself is contained in the Record Data field, and has the format shown in Table 3-2.

Table 3-2 – Media Identifier Format for DVD-RAM

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved: 0000_2				Type: 0000_2			
1	Manufacturer ID							
2								
3	Serial Number							
4								
5								
6								
7								

Within byte 0, the most significant 4 bits are reserved for future use, and are currently defined to have a value of zero. For forward compatibility, a non-zero value in these 4 bits shall not be considered an error. The least significant 4 bits of byte 0 are set according to the media type, and are defined to be 0000_2 for DVD-RAM. The 4C Entity, LLC assigns each licensee a unique 2-byte value to use in the Manufacturer ID field. Each licensee assigns 5-byte values to the Serial Number field that are unique for each piece of compliant DVD-RAM media that it manufactures.

3.2 Media Key Block (MKB)

CPRM compliant DVD-RAM media shall contain an MKB and an MKB Descriptor (described later), that are referred to together as the MKB Frame. The media manufacturer places the MKB Frame in the Control Data Area of the lead-in area's embossed data zone. The layout of the Control Data Area is shown in Table 3-3.

Table 3-3 – Layout of Control Data Area

ECC Blocks	Sectors		
	0-1	2-3	4-15
0-15	Already Defined	Reserved	MKB Pack #0
			...
			MKB Pack #15
16-31			MKB Pack #0
			...
			MKB Pack #15
...			...
176-191			MKB Pack #0
			...
			MKB Pack #15

The Control Data Area consists of 192 ECC Blocks of 16 sectors each. The first two sectors (Sectors 0 and 1) of each ECC Block have uses already defined by the DVD Forum. The next two sectors (Sectors 2 and 3) are reserved for future use. The remaining 12 sectors (Sectors 4 through 15) are available for storage of the MKB Frame. The 192 ECC Blocks of the Control Data Area are logically divided into 12 groups of 16 ECC Blocks each. Each group of 16 ECC Blocks contains identical data, meaning that the data is repeated 12 times for data integrity purposes. Sectors 4 through 15 of each ECC Block form a 24,576-byte data unit referred to as an MKB Pack. In all there are 16 MKB Packs, each repeated 12 times.

The MKB Frame is constructed from the data contained in the first n MKB Packs, where n depends on the size of the MKB Frame, and is at least 1 and at most 16. The bytes in the n MKB Packs are concatenated, in order, to form the MKB Frame. The first n-1 MKB Packs shall be used completely; the n^{th} MKB Pack may end with unused bytes, which are zero-filled. Figure 3-2 shows the formation of an MKB Frame in a case where n is 3.

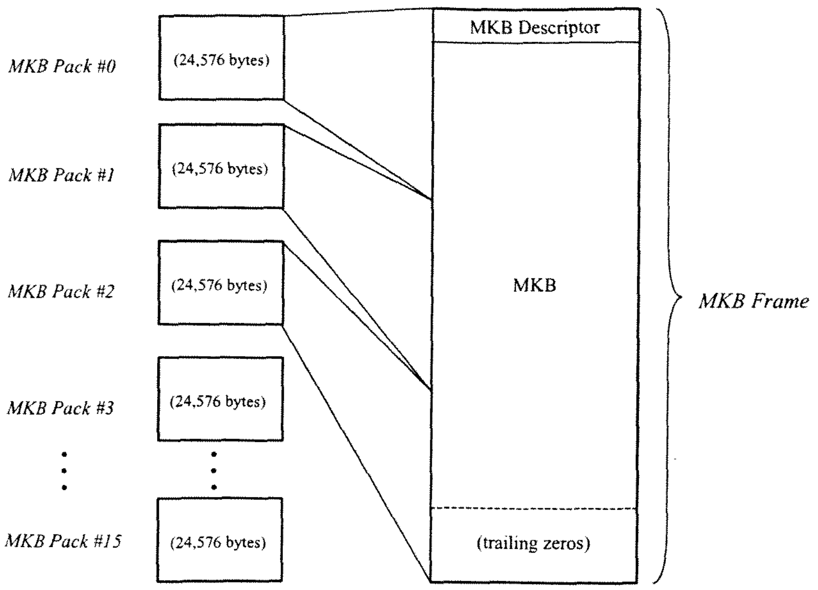


Figure 3-2 – Formation of an MKB Frame from 3 MKB Packs

The MKB Frame begins with a 16-byte MKB Descriptor, which is formatted as shown in Table 3-4.

Table 3-4 – Format of MKB Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	MKB_Hash							
:								
7								
8	Reserved: 0000000000000000_{16}							
:								
15								

The MKB_Hash field contains an 8-byte hash covering the MKB and any trailing zeros that may follow it (i.e. covering the entire MKB Frame, except for the MKB Descriptor), and is calculated as

MKB_Hash = C2_H(MKB and trailing zeros).

The MKB_Hash is used to ensure the integrity of the MKB when it is transferred from a drive to a host using authentication, as described in Chapter 6 of this document. The final 8 bytes of the MKB Descriptor are reserved for future use, and are currently defined to have values of zero. For forward compatibility, non-zero values in these bytes shall be ignored.

The rest of the MKB Frame consists of the MKB itself, which is formatted as described in the *Introduction and Common Cryptographic Elements* book of this specification, possibly followed by trailing zeros. For the first generation, there may be at most 16 MKB Packs, allowing for a maximum MKB size of 16 × 24,576 - 16 = 393,200 bytes. For the first-generation DVD-RAM MKB, 16 Device Key Columns are defined, and a given Column can have at most 4096 Rows. Media Key Blocks for use on DVD-RAM media are provided by the 4C Entity, LLC, and shall be updated periodically on newly manufactured media as described in the CPRM license agreement.

The number of MKB Packs used to construct the MKB Frame is determined using a field of the Copyright Management Information (CPR_MAI) table. The disc manufacturer pre-records the CPR_MAI table in each of the sector headers of relative sector numbers 2 through 15 of each ECC Block in the Control Data Area. Table 3-5 shows the format of the CPR_MAI table.

Table 3-5 – CPR_MAI Table Format

Bit Byte	7	6	5	4	3	2	1	0
0	Copyright Protection System Type (CPS_TY): 02_{16}							
1	Reserved							
2	CPRM Version: 01_{16}							
3	Total MKB Packs Used							
4	Reserved				CPRM Authentication Control Code			
5	Reserved							

The CPS_TY field contains the value 02_{16}, indicating that the disc contains data structures for CPRM (i.e. is CPRM compliant). Other possible values for CPS_TY are currently reserved. The CPRM Version field value is currently defined as 01_{16}. The Total MKB Packs Used field indicates the number of MKB Packs to be used in constructing the MKB Frame. The CPRM Authentication Control Code field is used in conjunction with the authentication scheme referred to in Chapter 6 of this document. The value for use in this field is provided by the 4C Entity, LLC, and is subject to change upon notice. When an updated value is provided, that new value must be included on newly manufactured media at or before such time that updated Media Key Blocks are next included on such media (see the CPRM license agreement for requirements on updating Media Key Blocks on newly manufactured media).

This page is intentionally left blank.

Chapter 4
CPRM Components on DVD-R and DVD-RW Media

4. Introduction

This chapter specifies the location and format details of the common CPRM components described in the *Introduction and Common Cryptographic Elements* book of this specification, when stored on DVD-R and DVD-RW media. In this document, "DVD-R" refers solely to "DVD-R for General" media. The DVD-R and DVD-RW formats are the subject of a license from the DVD Forum, which also publishes specifications describing the format in detail (see the corresponding references in Section 1.3):

- DVD Specifications for Recordable Disc for General, Part 1: Physical Specifications
- DVD Specifications for Recordable Disc for General, Part 2: File System Specifications
- DVD Specifications for Re-recordable Disc, Part 1: Physical Specifications
- DVD Specifications for Re-recordable Disc, Part 2: File System Specifications

This chapter assumes the reader is familiar with the DVD-R and DVD-RW formats, and focuses on those aspects of the format that are relevant to CPRM protection. Figure 4-1 gives an overview of the locations of CPRM related components on DVD-R and DVD-RW media.

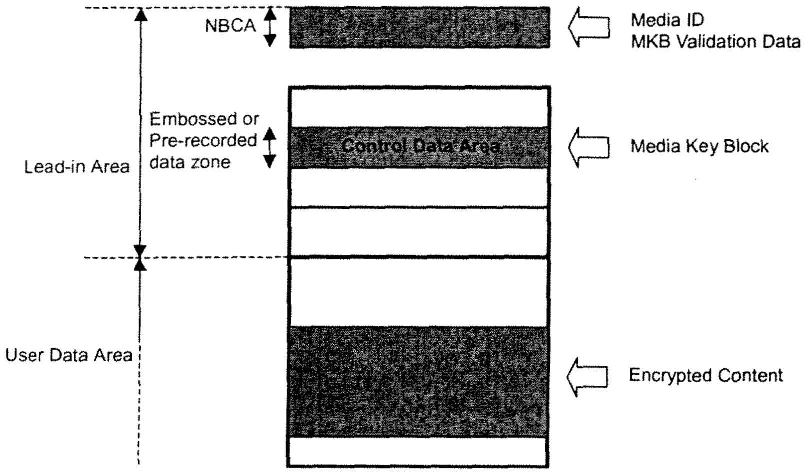


Figure 4-1 – Physical Layout of Common CPRM Components on DVD-R and DVD-RW Media

- A Media Identifier (ID_{media}) is pre-recorded in the Narrow Burst Cutting Area (NBCA).
- A Media Key Block (MKB) Validation Data is pre-recorded in the Narrow Burst Cutting Area (NBCA).
- A Media Key Block (MKB) is pre-recorded in the Embossed or Pre-recorded data zone of the Lead-in Area.
- Encrypted Content is recorded in the User Data Area.

In addition, other application-specific components related to CPRM may also be stored in the User Data Area, as described later in the chapters of this document covering application formats.

The remainder of this chapter contains further details on the location and format of the Media Identifier, MKB Validation Data and MKB. DVD-R and DVD-RW media containing a Media Identifier, MKB Validation Data and MKB as described in this chapter will be referred to as CPRM compliant DVD-R and DVD-RW media.

4.1 Media Identifier and MKB Validation Data

CPRM compliant DVD-R and DVD-RW media shall contain a 64-bit Media Identifier (ID_{media}) and 16-byte MKB Validation Data, which are placed in the Narrow Burst Cutting Area (NBCA) by the media manufacturer. The NBCA can contain multiple, contiguous blocks of data, called BCA Records, each containing information for a different use. Each BCA Record begins with a 2-byte BCA Record ID field identifying the Record's use, followed by a 1-byte Version Number field, followed by a 1-byte Data Length field indicating the length, in bytes, of the remaining data in the Record. Devices must not assume a fixed location or size for a given BCA Record, and must instead use the BCA Record ID and Data Length fields to go from one Record to the next until the desired Record is found. For CPRM compliant DVD-R and DVD-RW media, the NBCA shall include a BCA Record containing the Media Identifier and another BCA Record containing the MKB Validation Data, with format as shown in Table 4-1.

Table 4-1 – Format of BCA Records Containing the Media ID and MKB Validation Data

Bit Byte	7	6	5	4	3	2	1	0
0	(msb) BCA Record ID: 0002$_{16}$							
1								(lsb)
2	Version Number: 01$_{16}$							
3	Data Length: 08$_{16}$							
4	(msb) Record Data: Media Identifier							
:								
11								(lsb)
12	(msb) BCA Record ID: 0003$_{16}$							
13								(lsb)
14	Version Number: 01$_{16}$							
15	Data Length: 10$_{16}$							
16	(msb) Record Data: MKB Validation Data							
:								
:								
:								
:								
31								(lsb)

The BCA Record ID field identifies the use for the BCA Record, with the value 0002$_{16}$ indicating a Media Identifier Record and the value 0003$_{16}$ indicating a MKB Validation Data Record. For the Media Identifier Record, the Version Number field is currently defined as 01$_{16}$. The Data Length field indicates the length in bytes of the subsequent Record Data field, which is 08$_{16}$ for the Media Identifier Version 01$_{16}$. The Media Identifier itself is contained in the Record Data field, and has the format shown in Table 4-2 for DVD-R and Table 4-3 for DVD-RW. For the MKB Validation Data Record, the Version Number field is currently defined as 01$_{16}$. The Data Length field indicates the length in bytes of the subsequent Record Data field, which is 10$_{16}$ for the MKB Validation Data Version 01$_{16}$. The MKB Validation Data itself is contained in the Record Data field, and has the format shown in Table 4-4.

Table 4-2 – Media Identifier Format for DVD-R

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved: 0000_2				Type: 0001_2			
1	Manufacturer ID							
2								
3	Serial Number							
4								
5								
6								
7								

Within byte 0, the most significant 4 bits are reserved for future use, and are currently defined to have a value of zero. For forward compatibility, a non-zero value in these 4 bits shall not be considered an error. The least significant 4 bits of byte 0 are set according to the media type, and are defined to be 0001_2 for DVD-R. The 4C Entity, LLC assigns each licensee a unique 2-byte value to use in the Manufacturer ID field. Each licensee assigns 5-byte values to the Serial Number field that are unique for each piece of compliant DVD-R media that it manufactures.

Table 4-3 – Media Identifier Format for DVD-RW

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved: 0000_2				Type: 0010_2			
1	Manufacturer ID							
2								
3	Serial Number							
4								
5								
6								
7								

Within byte 0, the most significant 4 bits are reserved for future use, and are currently defined to have a value of zero. For forward compatibility, a non-zero value in these 4 bits shall not be considered an error. The least significant 4 bits of byte 0 are set according to the media type, and are defined to be 0010_2 for DVD-RW. The 4C Entity, LLC assigns each licensee a unique 2-byte value to use in the Manufacturer ID field. Each licensee assigns 5-byte values to the Serial Number field that are unique for each piece of compliant DVD-RW media that it manufactures.

Table 4-4 – MKB Validation Data Format for DVD-R and DVD-RW

Byte \ Bit	7	6	5	4	3	2	1	0
0	MKB_Hash							
:								
7								
8	MKB Verification Data (D_v)							
:								
15								

The MKB_Hash field contains an 8-byte hash covering the MKB and any trailing zeros that may follow it (i.e. covering the entire MKB Frame, except for the MKB Descriptor, both of which are described in Section 4.2), and is calculated as

MKB_Hash = C2_H(MKB and trailing zeros).

The MKB_Hash is used to ensure the integrity of the MKB when it is transferred from a drive to a host using authentication, as described in Chapter 6 of this document. Note that some CPRM compliant DVD-RW media may have been manufactured with an MKB_Hash value that was calculated using a different formula than that described above. See Section 6.1 regarding host validation of the MKB acquired from such media.

The MKB Verification Data (D_v) field contains an 8-byte value that is exactly the same as the value contained in the Verification Data field of the Verify Media Key Record in the MKB, i.e.

$D_v = \text{C2\_E}(K_m, \text{DEADBEEF}_{16} \,||\, \text{XXXXXXXX}_{16})$

where K_m is the correct final Media Key value, and XXXXXXXX_{16} is an arbitrary 4-byte value.

A device that does not use the drive-host authentication described in Chapter 6 shall verify the authenticity of the Media Key calculated from the MKB, by reading this D_v value from the NBCA and using it to verify the condition

$[\text{C2\_D}(K_m, D_v)]_{msb\_32} == \text{DEADBEEF}_{16}$

where K_m is the Media Key value calculated by processing the MKB as described in the *Introduction and Common Cryptographic Elements* book of this specification.

The device shall not use K_m for playback or recording of CPRM encrypted content until this condition is successfully verified. Note that the Verification Data field of the Verify Media Key Record in the MKB itself shall not be used to verify the authenticity of the Media Key.

4.2 Media Key Block (MKB)

CPRM compliant DVD-R and DVD-RW media shall contain an MKB and an MKB Descriptor (described later), that are referred to together as the MKB Frame. The media manufacturer places the MKB Frame in the Control Data Area of the lead-in area's embossed or pre-recorded data zone. The layout of the Control Data Area is shown in Table 4-5.

Table 4-5 – Layout of Control Data Area

ECC Blocks	Sectors		
	0-1	2-3	4-15
0-15	Already Defined	Reserved	MKB Pack #0
			...
			MKB Pack #15
16-31			MKB Pack #0
			...
			MKB Pack #15
...			...
160-175			MKB Pack #0
			...
			MKB Pack #15

The Control Data Area contains 176 ECC Blocks of 16 sectors each to store the MKB. The first two sectors (Sectors 0 and 1) of each ECC Block have uses already defined by the DVD Forum. The next two sectors (Sectors 2 and 3) are reserved for future use. The remaining 12 sectors (Sectors 4 through 15) are available for storage of the MKB Frame. The 176 ECC Blocks of the Control Data Area are logically divided into 11 groups of 16 ECC Blocks each. Each group of 16 ECC Blocks contains identical data, meaning that the data is repeated 11 times for data integrity purposes. Sectors 4 through 15 of each ECC Block form a 24,576-byte data unit referred to as an MKB Pack. In all there are 16 MKB Packs, each repeated 11 times.

The MKB Frame is constructed from the data contained in the first n MKB Packs, where n depends on the size of the MKB Frame, and is at least 1 and at most 16. The bytes in the n MKB Packs are concatenated, in order, to form the MKB Frame. The first n-1 MKB Packs shall be used completely; the nth MKB Pack may end with unused bytes, which are zero-filled. Figure 4-2 shows the formation of an MKB Frame in a case where n is 3.

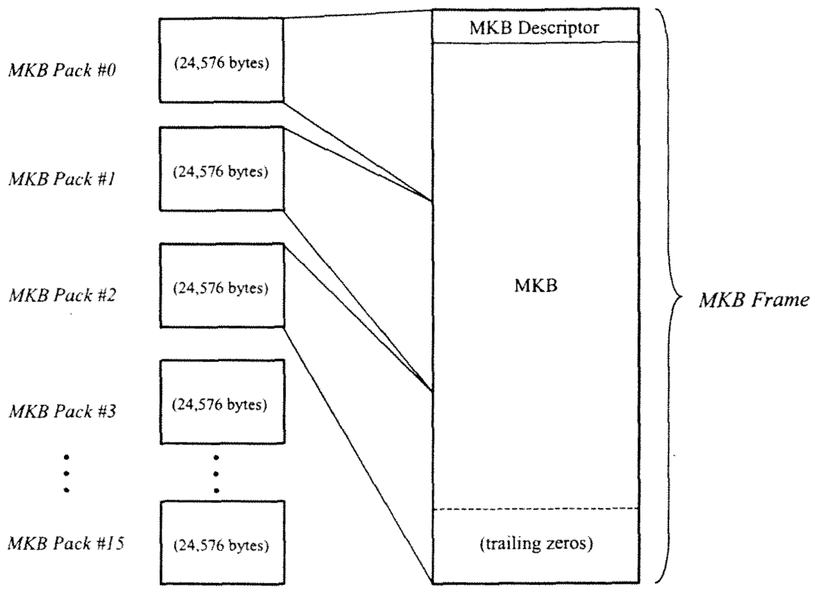


Figure 4-2 – Formation of an MKB Frame from 3 MKB Packs

The MKB Frame begins with a 16-byte MKB Descriptor, which is formatted as shown in Table 4-6.

Table 4-6 – Format of MKB Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved: 0000000000000000_{16}							
:								
7								
8	Reserved: 0000000000000000_{16}							
:								
15								

The MKB Descriptor for DVD-R and DVD-RW media does not contain the MKB_Hash, instead the first 8 bytes are reserved and are currently defined to have values of zero. The final 8 bytes of the MKB Descriptor are reserved for future use, and are currently defined to have values of zero. For forward compatibility, non-zero values in these bytes shall be ignored.

The rest of the MKB Frame consists of the MKB itself, which is formatted as described in the *Introduction and Common Cryptographic Elements* book of this specification, possibly followed by trailing zeros. For the first generation, there may be at most 16 MKB Packs, allowing for a maximum MKB size of 16 × 24,576 - 16 = 393,200 bytes. For the first-generation DVD-R and DVD-RW MKB, 16 Device Key Columns are defined, and a given Column can have at most 4096 Rows. Media Key Blocks for use on DVD-R and DVD-RW media are provided by the 4C Entity, LLC, and shall be updated periodically on newly manufactured media as described in the CPRM license agreement.

The number of MKB Packs used to construct the MKB Frame is determined using a field of the Copyright Management Information (CPR_MAI) table. The disc manufacturer pre-records the CPR_MAI table in each of the sector headers of relative sector numbers 2 through 15 of each ECC Block in the Control Data Area. Table 4-7 shows the format of the CPR_MAI table.

Table 4-7 – CPR_MAI Table Format

Bit Byte	7	6	5	4	3	2	1	0
0	Copyright Protection System Type (CPS_TY): 02_{16}							
1	Reserved							
2	CPRM Version: 01_{16}							
3	Total MKB Packs Used							
4	Reserved				CPRM Authentication Control Code			
5	Reserved							

The CPS_TY field contains the value 02_{16}, indicating that the disc contains data structures for CPRM (i.e. is CPRM compliant). Other possible values for CPS_TY are currently reserved. The CPRM Version field value is currently defined as 01_{16}. The Total MKB Packs Used field indicates the number of MKB Packs to be used in constructing the MKB Frame. The CPRM Authentication Control Code field is used in conjunction with the authentication scheme referred to in Chapter 6 of this document. The value for use in this field is provided by the 4C Entity, LLC, and is subject to change upon notice. When an updated value is provided, that new value must be included on newly manufactured media at or before such time that updated Media Key Blocks are next included on such media (see the CPRM license agreement for requirements on updating Media Key Blocks on newly manufactured media).

This page is intentionally left blank.

Chapter 5
CPRM for the Video Recording Format

5. Introduction

This chapter describes the use of CPRM to protect content stored on CPRM compliant media of the types described in the previous chapters of this document, using the Video Recording format. The Video Recording format is defined by the DVD Forum for real-time recording (on Rewritable, Recordable and Re-recordable DVD media) of moving pictures and still pictures with associated audio. The Video Recording format is the subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.3):

- DVD Specifications for DVD-RAM/DVD-RW/DVD-R for General Discs, Part 3: Video Recording Specifications

This chapter assumes the reader is familiar with the Video Recording format, and focuses on those aspects of the format that are relevant to CPRM protection. Details provided include the locations of cryptographic elements within the format, and their use in CPRM cryptographic key management and encryption.

5.1 Stored Data Values Relevant to CPRM

For each disc, the Video Recording format uses a management information file named VR_MANGR.IFO. Included in this file is a 512-byte Video Manger Information Management Table (VMGI_MAT), part of which is used by CPRM to store a 64-bit Encrypted Title Key (K_{te}) and an associated Encrypted Title Key Status (K_{te}_Stat) bit, as shown in Table 5-1.

Table 5-1 – Storage of Encrypted Title Key in VMGI_MAT

Bit Byte	7	6	5	4	3	2	1	0
0	(Data defined in Video Recording specification)							
:								
263								
264	Reserved: 0							
265	Reserved: 0							
266	Reserved: 0							
267	Reserved: 0							K_{te}_Stat
268	K_{te}							
:								
275								
276	(Data defined in Video Recording Specification)							
:								
511								

Note that for Video Recording, there is a single K_{te} per volume. The usage of K_{te} is described in Section 5.2. The K_{te}_Stat field indicates the status of the K_{te} field, as shown in Table 5-2.

Table 5-2 – Encoding of K_{te}_Stat Field in VMGI_MAT

K_{te}_Stat value	Status of K_{te} field
0	No valid K_{te} value is present
1	A valid K_{te} value is present

The Video Recording format stores content stream data in stream data files. Content stream data is structured as a sequence of 2048-byte packs, which hold different information depending on the pack type. Real-time Data Information (RDI) packs carry real-time data information. Video packs, Audio packs, and Sub-picture packs carry audio-visual content, and are referred to generically in this chapter as AV Packs.

RDI packs occur periodically within a content stream (with presentation times at least 0.4 seconds and at most 1.0 seconds apart), and are used to carry various types of information about the stream. RDI packs are not encrypted. Table 5-3 shows an RDI pack.

Table 5-3 – RDI Pack

	Bit Byte	7	6	5	4	3	2	1	0
	0 : 60	(Data defined in Video Recording specification)							
DCI_CCI	61 : 67	(Data defined in Video Recording specification)							
	68	CGMS		APSTB			EPN		
	69 : 2039	(Data defined in Video Recording specification)							
	2040 : 2047	DCI_CCI Verification Data							

The data field values in a given RDI pack apply to subsequent AV Packs in the recorded content stream, up to the occurrence of the next RDI pack or the end of the stream. The data field values may change from one RDI pack to another. The APSTB field indicates the analog protection status of corresponding AV Packs, with encodings defined in the Video Recording specification. The CGMS, EPN and DCI_CCI Verification Data fields together indicate the copy control status of corresponding AV Packs, as shown in Table 5-4 and as described below.

Table 5-4 – Indication of Copy Control Status

CGMS	EPN	DCI_CCI Verification Data Verified?	Content Status
00_2	-	-	Copy freely
11_2	0	-	No more copies
11_2	1	No	No more copies
11_2	1	Yes	Protected using CPRM, but copy control restrictions not asserted

For content recorded without CPRM protection, Recording Devices shall set the CGMS field corresponding to that content in the recorded stream to 00_2, and shall not encrypt the corresponding AV Packs. For content recorded with CPRM protection, Recording Devices shall set the CGMS field corresponding to that content in the recorded stream to 11_2, and shall encrypt all of the corresponding AV Packs as described in Section 5.2.1.

Where no copies of CPRM protected content are to be permitted, the EPN field corresponding to that content in the recorded stream shall be set to 0. Where copy control restrictions are not asserted with respect to such protected content, the EPN field shall be set to 1 and the DCI_CCI Verification Data field shall be set as described in Section 5.2.1. If a Playback Device does not successfully verify the DCI_CCI Verification Data as described in Section 5.2.2, that device shall treat the corresponding content as if the EPN field had a value of 0.

Since the CGMS field is not protected from malicious tampering (except where DCI_CCI Verification Data is present and verified), Playback Devices shall actually control copying of the recorded content based on whether it is encrypted using CPRM, as well as on the corresponding EPN and DCI_CCI Verification Data field values described above. Unencrypted content may be freely copied without any restriction or protection requirement. CPRM encrypted content with a corresponding EPN field value of 1 and a successfully verified DCI_CCI Verification Data field value may be copied without restriction provided that such copies are protected as required by the CPRM license agreement. Copying of CPRM encrypted content with a corresponding EPN field value of 0, or with a corresponding DCI_CCI Verification Data field value that was not successfully verified, is not authorized.

Table 5-5 shows an encrypted AV Pack.

Table 5-5 – Encrypted AV Pack

	Bit **Byte**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Unencrypted Portion (128 bytes)	0 : 19	(Data defined in Video Recording specification)							
	20			PES_scrambling_ Control					
	21 : 83	(Data defined in Video Recording specification)							
	84 : 91	Title Key Conversion Data (D_{tkc})							
	92 : 127	(Data defined in Video Recording specification)							
Encrypted Portion (1920 bytes)	128 : 2047	**Encrypted AV Data (D_{av_e})**							

For the Video Recording format, the 2-bit PES_scrambling_control field is set to 11_2 in an encrypted AV Pack, and 00_2 in an unencrypted AV Pack. The use of the 64-bit Title Key Conversion Data (D_{tkc}) is described in Section 5.2. The first 128 bytes of the pack are unencrypted. The final 1920 bytes, referred to as the Encrypted AV Data (D_{av_e}), are encrypted as described in Section 5.2.1. Before encryption (or after decryption), those same 1920 bytes are referred to as Unencrypted AV Data (D_{av_u}).

Table 5-6 summarizes stored data values that are relevant to CPRM protection of Video Recording formatted content.

Table 5-6 – Video Recording Stored Data Values Relevant to CPRM

Data Value	Size	Storage Location	Comment
Encrypted Title Key (K_{te})	64 bits	VR_MANGR.IFO	One per disc
Encrypted Title Key Status (K_{te}_Stat)	1 bit	VR_MANGR.IFO	Indicates status of K_{te}
DCI_CCI	64 bits	RDI Pack	Includes APSTB, CGMS and EPN fields
APSTB	2 bits	RDI Pack	Analog Protection Status
CGMS	2 bits	RDI Pack	Copy control information
EPN	1 bit	RDI Pack	EPN status
DCI_CCI Verification Data	64 bits	RDI Pack	DCI_CCI verification data
PES_scrambling_control	2 bits	Each encrypted AV Pack	–
Title Key Conversion Data (D_{tkc})	64 bits	Each encrypted AV Pack	–
Encrypted AV Data (D_{av_e})	1920 bytes	Each encrypted AV Pack	C2 C-CBC encryption frame

5.2 Content Encryption and Decryption

Figure 5-1 illustrates the process for encryption and decryption of Video Recording formatted content on CPRM compliant DVD media.

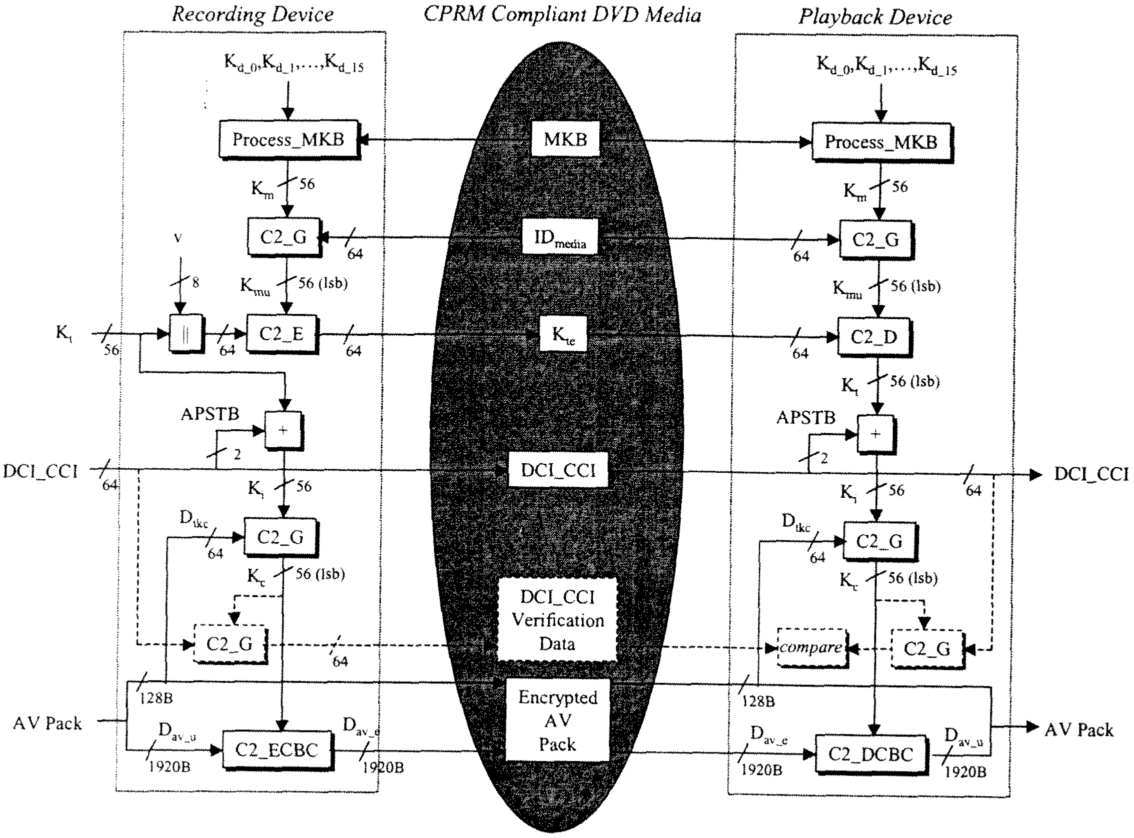


Figure 5-1 – Content Encryption and Decryption for the Video Recording Format

The remainder of this section describes the encryption and decryption processes in detail.

5.2.1 Content Encryption

The process to encrypt Video Recording formatted content is as follows:

1. Calculate Media Key (K_m):

The Recording Device reads the MKB from the disc, and uses its Device Keys ($K_{d\_0}, K_{d\_1}, \ldots, K_{d\_15}$) to calculate K_m as described in the *Introduction and Common Cryptographic Elements* book of this specification.

2. Calculate Media Unique Key (K_{mu}):

The Recording Device reads the Media Identifier (ID_{media}) from the disc, and calculates K_{mu} as

$K_{mu} = [C2\_G(K_m, ID_{media})]_{lsb\_56}$,

where C2_G represents the C2 One-way Function defined in the *Introduction and Common Cryptographic Elements* book of this specification.

3. Generate (or calculate) Title Key (K_t):

For the Video Recording format, a single 56-bit Title Key (K_t) is used for all titles recorded on a given disc.

The Recording Device examines the K_{te}_Stat field of the VMGI_MAT table to determine if an Encrypted Title Key (K_{te}) is already recorded on the disc. If a K_{te} is not already recorded on the disc (K_{te}_Stat == 0), the Recording Device generates K_t using a suitable random number generator as defined in the *Introduction and Common Cryptographic Elements* book of this specification.

If a K_{te} is already recorded on the disc (K_{te}_Stat == 1), the Recording Device calculates K_t using the same method that is used by a playback device (see Section 5.2.2, step 3). Note that the case where the Recording Device uses this step is not illustrated in Figure 5-1.

4. Calculate and record Encrypted Title Key (K_{te}):

If a K_{te} is already recorded on the disc (K_{te}_Stat == 1), this step is skipped.

Otherwise, the Recording Device selects an arbitrary 8-bit value v (any value is acceptable), and calculates K_{te} as

$K_{te} = C2\_E(K_{mu}, v \,||\, K_t)$,

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification.

The Recording Device records K_{te} on the disc (in the VMGI_MAT table), and sets the K_{te}_Stat bit to 1.

5. Calculate intermediate value K_i:

The Recording Device calculates the intermediate 56-bit value K_i by taking

$K_i = K_t + (0000000000000_{16} \,||\, 00_2 \,||\, APSTB)$

where + represents addition modulo 2^{56},

and then padding the result to 56 bits by prepending zero-valued bits as needed. The APSTB is recorded on the disc. This step is repeated whenever the APSTB value changes during the recording of encrypted content.

6. Encrypt AV Packs:

For each AV Pack to be encrypted, the Recording Device uses that pack's Title Key Conversion Data (D_{tkc}) to calculate a 56-bit Content Key (K_c) as follows:

$K_c = [C2\_G(K_i, D_{tkc})]_{lsb\_56}$.

The resulting K_c value is then used to encrypt that pack's 1920-byte Unencrypted AV Data (D_{av_u}) as follows:

$D_{av\_e} = C2\_ECBC(K_c, D_{av\_u})$,

where C2_ECBC represents encryption using the C2 cipher in C-CBC mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 1920-byte D_{av_u} encryption.

The PES_scrambling_control field of the encrypted AV Pack is set to 11_2.

7. For RDI packs with EPN == 1, calculate and record DCI_CCI Verification Data:

For each RDI pack with an EPN field value of 1, the Recording Device uses the 64-bit DCI_CCI field of that RDI pack, and the Content Key (K_c) of the AV Pack that is to be recorded immediately after that RDI pack, to calculate a 64-bit DCI_CCI Verification Data value as follows:

DCI_CCI Verification Data = C2_G(K_c, DCI_CCI).

The DCI_CCI Verification Data value is recorded on the disc, within that RDI pack.

5.2.2 Content Decryption

The process to decrypt encrypted Video Recording formatted content is as follows:

1. Calculate Media Key (K_m).

The Playback Device reads the MKB from the disc, and uses its Device Keys ($K_{d\_0}, K_{d\_1}, \ldots, K_{d\_15}$) to calculate K_m as described in the *Introduction and Common Cryptographic Elements* book of this specification.

2. Calculate Media Unique Key (K_{mu}):

The Playback Device reads the Media Identifier (ID_{media}) from the disc, and calculates K_{mu} as

$K_{mu} = [C2\_G(K_m, ID_{media})]_{lsb\_56}$.

3. Calculate Title Key (K_t):

The Playback Device reads the Encrypted Title Key (K_{te}) from the disc, and calculates K_t as

$K_t = [C2\_D(K_{mu}, K_{te})]_{lsb\_56}$,

where C2_D represents decryption using the C2 cipher in ECB mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification.

4. Calculate intermediate value K_i:

The Playback Device calculates the intermediate 56-bit value K_i by taking

$K_i = K_t + (0000000000000_{16} \,||\, 00_2 \,||\, APSTB)$

where + represents addition modulo 2^{56},

and then padding the result to 56 bits by prepending zero-valued bits as needed. This step is repeated whenever the APSTB value is changed in a subsequent RDI Pack.

5. Decrypt AV Packs:

For each AV Pack to be decrypted (i.e. having a PES_scrambling_control field value of 11_2), the Playback Device uses that pack's Title Key Conversion Data (D_{tkc}) to calculate a 56-bit Content Key (K_c) as follows:

$K_c = [C2\_G(K_i, D_{tkc})]_{lsb\_56}$.

The resulting K_c value is then used to decrypt that pack's 1920-byte Encrypted Data (D_{av_e}) as follows:

$D_{av\_u} = C2\_DCBC(K_c, D_{av\_e})$,

where C2_DCBC represents decryption using the C2 cipher in C-CBC mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 1920-byte D_{av_e} decryption.

6. For RDI packs with EPN == 1, check DCI_CCI Verification Data:

For each RDI pack with an EPN field value of 1, the Playback Device reads the DCI_CCI and DCI_CCI Verification Data fields of that RDI pack from the disc, and uses the Content Key (K_c) of the AV Pack recorded immediately after that RDI pack to verify the following condition:

$$C2\_G(K_c, DCI\_CCI) == DCI\_CCI \text{ Verification Data.}$$

If the condition is not successfully verified, the Playback Device shall treat the content corresponding to that RDI Pack as if the EPN field value of that RDI pack had been 0.

Chapter 6
PC Based System Architecture

6. Introduction

CPRM for recordable DVD media formats can be implemented in a PC based system. In such a system, a DVD drive and PC host act together as the Recording Device and/or Playback Device for CPRM protected content. The procedure for recording or playback of the content is the same as described in previous chapters of this document, except for additional steps that are required to enable the host to verify the integrity of the Media Key Block and Media Identifier values it receives from the drive. Figure 6-1 illustrates this procedure.

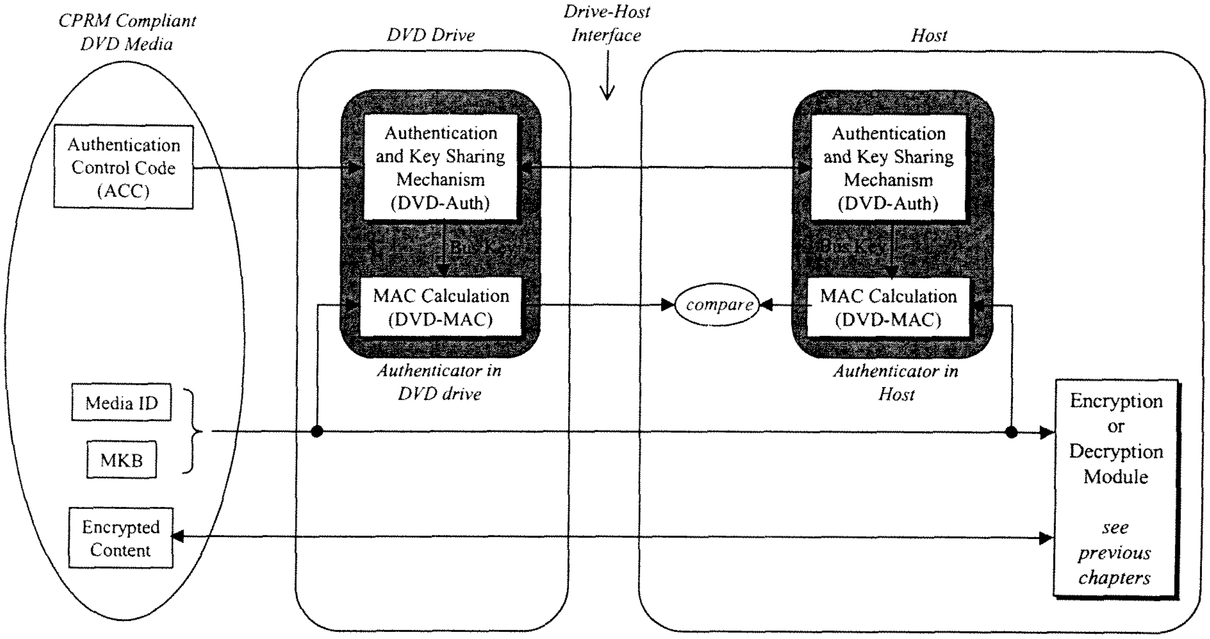

CPRM Compliant DVD Media
DVD Drive
Drive-Host Interface
Host
Authentication Control Code (ACC)
Authentication and Key Sharing Mechanism (DVD-Auth)
Bus Key
MAC Calculation (DVD-MAC)
Authenticator in DVD drive
compare
Authentication and Key Sharing Mechanism (DVD-Auth)
Bus Key
MAC Calculation (DVD-MAC)
Authenticator in Host
Media ID
MKB
Encrypted Content
Encryption or Decryption Module
see previous chapters

Figure 6-1 – Encryption and Decryption of CPRM Protected Content in a PC Based System

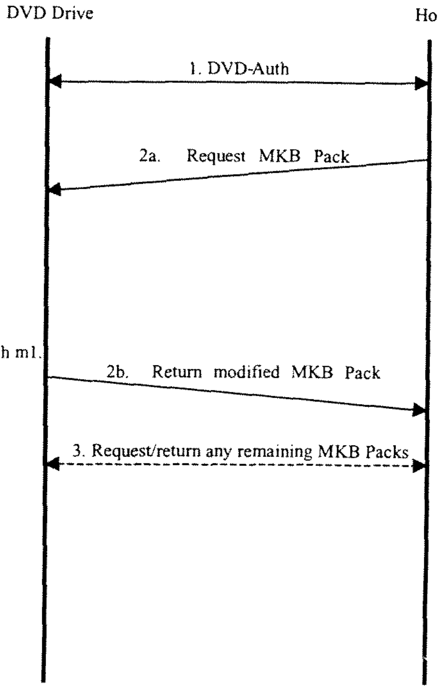
This procedure uses the DVD drive authentication algorithm already defined for use with the Content Scramble System (CSS) for DVD-Video, and a message authentication code (MAC) calculation algorithm based on the same underlying functions. A description of those algorithms (shown in the gray shaded areas) is available separately in the *CSS-based DVD Drive Authentication for CPRM* document cited in Section 1.3. Both that document and this document refer to those algorithms as:

- Authentication and Key Sharing (DVD-Auth)
- Message Authentication Code Calculation (DVD-MAC)

Note that neither the Media Key Block nor the Media Identifier needs to be kept confidential during transfer from the drive to the host. The purpose of the authentication and MAC calculation is only to enable the host to verify the integrity of those values. The remainder of this chapter describes in further detail the procedures used to verify the Media Key Block and Media Identifier integrity, as well as some extensions of the Mt. Fuji command set specification that support those procedures.

6.1 Protocol for Validating Media Key Block

Figure 6-2 shows the protocol flow whereby a host acquires the Media Key Block (MKB) stored on DVD-RAM media, and verifies the integrity of the received value.


DVD Drive
Host
1. DVD-Auth
2a. Request MKB Pack
2b. Return modified MKB Pack
3. Request/return any remaining MKB Packs

If DVD-Auth successful:

If DVD-Auth successful:

Read MKB Pack #0 from disc.

Using MKB_Hash field of MKB Descriptor,
Calculate m1 = DVD-MAC(MKB_Hash),
and replace first 10 bytes of MKB Descriptor with m1.

Calculate h = C2_H(MKB and trailing zeros), including any unused bytes that follow the MKB in the MKB Frame.

Calculate m2 = DVD-MAC(h).

Verify m1 == m2.

If fails, there could be an alternative verification as follows (see text below in this section)

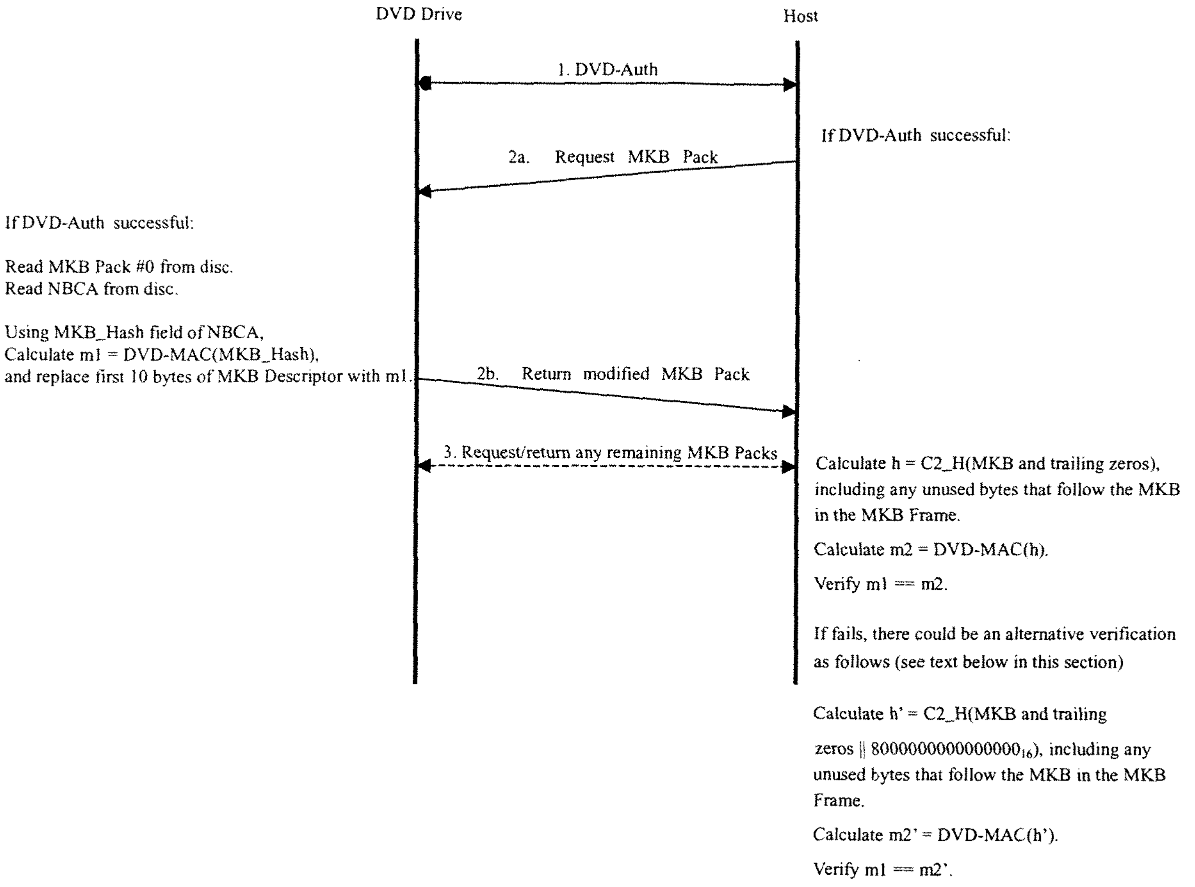
Calculate h' = C2_H(MKB and trailing zeros || 8000000000000000_{16}), including any unused bytes that follow the MKB in the MKB Frame.

Calculate m2' = DVD-MAC(h').

Verify m1 == m2'.

Figure 6-2 – Protocol Flow for Host Acquisition and Validation of MKB from DVD-RAM Media

Figure 6-3 shows the protocol flow whereby a host acquires the Media Key Block (MKB) stored on DVD-R and DVD-RW media, and verifies the integrity of the received value.


DVD Drive
Host
1. DVD-Auth
2a. Request MKB Pack
2b. Return modified MKB Pack
3. Request/return any remaining MKB Packs

If DVD-Auth successful:

If DVD-Auth successful:

Read MKB Pack #0 from disc.
Read NBCA from disc.

Using MKB_Hash field of NBCA,
Calculate m1 = DVD-MAC(MKB_Hash),
and replace first 10 bytes of MKB Descriptor with m1.

Calculate h = C2_H(MKB and trailing zeros), including any unused bytes that follow the MKB in the MKB Frame.

Calculate m2 = DVD-MAC(h).

Verify m1 == m2.

If fails, there could be an alternative verification as follows (see text below in this section)

Calculate h' = C2_H(MKB and trailing zeros || 8000000000000000_{16}), including any unused bytes that follow the MKB in the MKB Frame.

Calculate m2' = DVD-MAC(h').

Verify m1 == m2'.

Figure 6-3 – Protocol Flow for Host Acquisition and Validation of MKB from DVD-R and DVD-RW Media

In all cases of recordable DVD media, the drive and host carry out the Authentication and Key Sharing (DVD-Auth) procedure (1), as described in the *CSS-based DVD Drive Authentication for CPRM* document. One input to the DVD-Auth procedure is the Authentication Control Code (ACC). For CPRM compliant DVD recordable media, the drive acquires this value from the CPRM Authentication Control Code field of the CPR_MAI table, described in Section 3.2 and Section 4.2. If the DVD-Auth procedure is successful, the drive and host calculate a shared Bus Key, and proceed with the remaining steps.

In the case of DVD-RAM media, upon request from the host (2a), the drive reads MKB Pack #0 from the media, and uses the MKB_Hash field of the MKB Descriptor to calculate the 80-bit value m1 as

> m1 = DVD-MAC(MKB_Hash),
>
> where DVD-MAC is the MAC calculation algorithm described in the *CSS-based DVD Drive Authentication for CPRM* document.

The drive then replaces the first 10 bytes of the MKB Descriptor with m1, and returns the modified MKB Pack #0 to the host (2b).

In the case of DVD-R and DVD-RW media, upon request from the host (2a), the drive reads MKB Pack #0 and the NBCA from the media, and uses the MKB_Hash field of the NBCA to calculate the 80-bit value m1 as m1 = DVD-MAC(MKB_Hash),

where DVD-MAC is the MAC calculation algorithm described in the *CSS-based DVD Drive Authentication for CPRM* document.

The drive then replaces the first 10 bytes of the MKB Descriptor with m1, and returns the modified MKB Pack #0 to the host (2b).

In all cases of recordable DVD media, if there are more MKB Packs available, the host reads them from the drive (3). Then, using the MKB and any unused (zero-valued) bytes that follow it in the MKB Frame, the host calculates the 64-bit value h as

h = C2_H(MKB and trailing zeros),

where C2_H represents the C2 Hash Function, as defined in the *Introduction and Common Cryptographic Elements* book of this specification.

Using the resulting h value, the host then calculates the 80-bit value m2 as

m2 = DVD-MAC(h).

The host shall verify the integrity of the received MKB (verify m1 == m2) before the calculation of the Media Unique Key (K_{mu}) described in previous chapters of this document.

In the case of DVD-RW media, or where a host implementation does not distinguish DVD-RW media from DVD-R and DVD-RAM media, if the first verification fails, the host shall perform an alternative verification by using an additional 8-byte value. In this case, the host calculates the 64-bit value h' as

h' = C2_H(MKB and trailing zeros || 8000000000000000_{16}),

where C2_H represents the C2 Hash Function, as defined in the *Introduction and Common Cryptographic Elements* book of this specification,

and using the resulting h' value, the host then calculates the 80-bit value m2' as

m2' = DVD-MAC(h'),

and the host then verifies the integrity of the received MKB (verify m1 == m2') before the calculation of the Media Unique Key (K_{mu}) described in previous chapters of this document.

If neither the first verification, nor the alternative verification, if applicable, is successful, the host shall abort the playback or recording session in progress. Note that whether the host verifies the MKB's integrity before or after the calculation of the Media Key (K_m) described in previous chapters of this document is implementation-defined.

6.2 Protocol for Validating Media Identifier

Figure 6-4 shows the protocol flow whereby a host acquires the Media Identifier (ID_{media}) stored on recordable DVD media, and verifies the integrity of the received value.

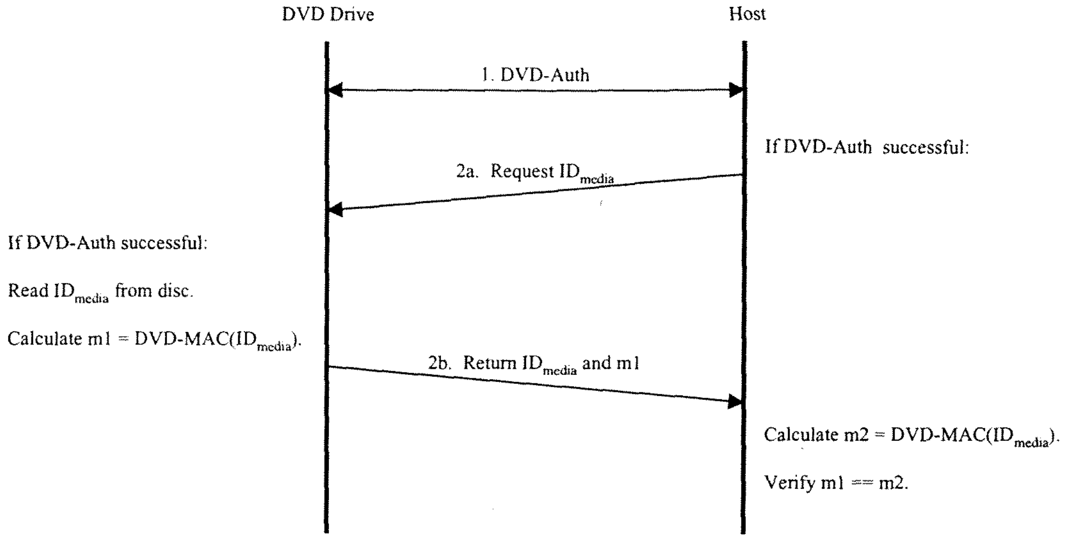

DVD Drive
Host
1. DVD-Auth
If DVD-Auth successful:
2a. Request ID_{media}
If DVD-Auth successful:
Read ID_{media} from disc.
Calculate m1 = DVD-MAC(ID_{media}).
2b. Return ID_{media} and m1
Calculate m2 = DVD-MAC(ID_{media}).
Verify m1 == m2.

Figure 6-4 – Protocol Flow for Host Acquisition and Validation of ID_{media}

The drive and host carry out the Authentication and Key Sharing (DVD-Auth) procedure (1), as described in the *CSS-based DVD Drive Authentication for CPRM* document. One input to the DVD-Auth procedure is the Authentication Control Code (ACC). For CPRM compliant DVD recordable media, the drive acquires this value from the CPRM Authentication Control Code field of the CPR_MAI table, described in Section 3.2 and Section 4.2. If the DVD-Auth procedure is successful, the drive and host calculate a shared Bus Key, and proceed with the remaining steps.

Upon request from the host (2a), the drive reads the ID_{media} value from the media, and uses it to calculate the 80-bit value m1 as

$$m1 = \text{DVD-MAC}(ID_{media}).$$

The drive then returns the ID_{media} and m1 values to the host (2b).

Using the received ID_{media} value, the host calculates the 80-bit value m2 as

$$m2 = \text{DVD-MAC}(ID_{media}).$$

The host shall verify the integrity of the received ID_{media} (verify m1 == m2) before the calculation of the Media Unique Key (K_{mu}) described in previous chapters of this document. If the verification fails, the host shall abort the playback or recording session in progress.

6.3 Mt. Fuji DVD Command Extensions for CPRM

The Mt. Fuji specification (see the corresponding reference in Section 1.3) defines commands and related structures used to control DVD drives (logical units). This section describes extensions to that specification for logical units that support CPRM functionality. Some additional information that is not found in the Mt. Fuji specification is also given, including the precise format of CPRM data values returned by the logical unit.

6.3.1 DVD CPRM Feature

The Mt. Fuji specification defines a number of Features, which are sets of commands, mode pages, and behaviors or operations supported by a logical unit. Features implemented by a logical unit are reported to the host via the GET CONFIGURATION command. This command can be used to identify all possible Features, as well those Features that are current (i.e. currently available, which may depend on factors such as the type of media currently loaded). A DVD Feature for CPRM is defined as shown in Table 6-1.

Table 6-1 – DVD CPRM Feature

Feature Code	Feature Name	Description	Mandatory Commands
$010B_{16}$	DVD CPRM	Ability to perform CPRM key management	REPORT KEY, SEND KEY, READ DVD STRUCTURE (Format Codes 06_{16} and 07_{16})

The DVD CPRM Feature Descriptor, obtained via the GET CONFIGURATION command, is shown in Table 6-2.

Table 6-2 – DVD CPRM Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(msb) Feature Code = $010B_{16}$							
1								(lsb)
2	Reserved		Version				Persistent	Current
3	Additional Length = 04_{16}							
4	Reserved							
5	Reserved							
6	Reserved							
7	CPRM version							

The **Current** bit, when set to zero, indicates that this Feature is not currently active. When set to one, the Feature is active. The DVD CPRM Feature shall be active if and only if a CPRM compliant DVD disc is loaded, which a CPRM compliant drive determines by confirming that at least the following conditions are true:

- The disc is a DVD-RAM, DVD-R or DVD-RW disc.
- The disc contains a CPR_MAI table in the Control Data Area that has a CPS_TY field value of 02_{16} and a Total MKB Packs Used field with a non zero value (see Section 3.2 or 4.2).
- The disc contains a BCA Record that has a BCA Record ID field value of 0002_{16} and a Data Length field value of at least 08_{16} (see Section 3.1 or 4.1).
- For a DVD-R or DVD-RW disc, the disc contains a BCA Record with a BCA Record ID field value of 0003_{16} (see Section 4.1).

The Feature Descriptor's **CPRM version** field shall be set to the value of the CPRM Version field of the CPR_MAI table.

The other fields of the Feature Descriptor shall be set as described in the Mt. Fuji specification.

6.3.2 REPORT KEY Command Extensions

The REPORT KEY Command requests the start of the authentication process, and provides data necessary for authentication and for generating a Bus Key for the DVD Logical Unit.

Table 6-3 – REPORT KEY Command

Bit Byte	7	6	5	4	3	2	1	0
0	Operation code ($A4_{16}$)							
1	LUN (Obsolete)			Reserved				
2	(msb)	Reserved/Logical Address						
3								
4								
5								(lsb)
6	Reserved							
7	Key Class							
8	(msb)	Allocation Length						
9								(lsb)
10	AGID		Key Format					
11	Vendor-Specific		Reserved			NACA	Flag	Link

The **Key Format** field indicates the type of information that is requested to be sent to the host.

Since a Bus Key is used in the transfer of the Media ID and Media Key Block, a new Key Format is defined for requesting an Authentication Grant ID for use in authentication prior to the transfer of those values, as shown in Table 6-4.

Table 6-4 – Key Format Code Definition for Requesting an AGID for CPRM

Key Format	Returned Data	Description	AGID Use
010001_2	AGID for CPRM	Returns an AUTHENTICATION GRANT ID for Authentication for CPRM (DVD-Auth)	Reserved & N/A

Table 6-5 shows the format of the data returned by the REPORT KEY command when Key Format 010001_2 is used.

Table 6-5 – REPORT KEY Data Format (with Key Format = 010001_2, Key Class = 0)

Bit Byte	7	6	5	4	3	2	1	0
0	(msb)	REPORT KEY Data Length (0006_{16})						
1								(lsb)
2	Reserved							
3	Reserved							
4	Reserved							
5	Reserved							
6	Reserved							
7	AGID		Reserved					

This Key Format requests the logical unit to return an Authentication Grant ID for CPRM. After a CPRM Authentication Grant ID is obtained, the DVD-Auth procedure defined in the *CSS-based DVD Drive Authentication for CPRM* document can be carried out, using the REPORT KEY and SEND KEY commands as described in the Mt. Fuji specification. The resulting Bus Key is used in the validated transfer of *only* the Media Identifier and Media Key Block (and *not* any other data such as CSS-related key data), as described previously in Sections 6.1 and 6.2, and as supported by the READ DVD STRUCTURE command extensions described in the next section.

6.3.3 READ DVD STRUCTURE Command Extensions

Logical units that implement the DVD CPRM Feature support extensions to the READ DVD STRUCTURE command. The READ DVD STRUCTURE command, shown in Table 6-6, requests that the Logical Unit transfer data from areas on the DVD media to the host.

Table 6-6 – READ DVD STRUCTURE Command

Bit Byte	7	6	5	4	3	2	1	0
0	Operation code (AD_{16})							
1	LUN (Obsolete)			Reserved				
2	(msb)							
3	Address							
4								
5								(lsb)
6	Layer Number							
7	Format							
8	(msb) Allocation Length							
9								(lsb)
10	AGID		Reserved					
11	Vendor-Specific		Reserved			NACA	Flag	Link

The **Format** field indicates the type of information that is requested by the host. New **Format** values defined for CPRM are shown in

Table 6-7, along with corresponding usage of the **Layer Number** and **Address** fields.

Table 6-7 – CPRM Format Code definitions for READ DVD STRUCTURE command

Format Code	Returned Data	Layer Number Field Usage	Address Field Usage	Description
06_{16}	Media Identifier	Reserved	Reserved	Returns the CPRM Media Identifier and a validating MAC.
07_{16}	Media Key Block	Reserved	Pack number	Returns the CPRM Media Key Block Pack data and a validating MAC.

For **Format** code 06_{16}, or **Format** code 07_{16} with the **Address** field set to 00000000_{16}, the returned data includes a message authentication code (MAC) that is calculated using a Bus Key, as described in the *CSS-based DVD Drive Authentication for CPRM* document. The host establishes the Bus Key via the DVD-Auth procedure, using the same command sequence that is used for CSS (via the REPORT KEY and SEND KEY commands, beginning with REPORT KEY Key Format = 010001_2) prior to calling the READ DVD STRUCTURE command. The READ DVD STRUCTURE command **AGID** field identifies the Authentication Grant ID that was used in establishing the Bus Key.

For **Format** code 07_{16}, the **Address** field is used to specify which MKB Pack is to be read. This field enables the host to read a Media Key Block Frame contained in multiple Packs.

The other fields of the READ DVD STRUCTURE command shall be set as described in the Mt. Fuji specification.

6.3.3.1 MEDIA IDENTIFIER (Format 06_{16})

Table 6-8 – READ DVD STRUCTURE Data Format (With Format Field = 06_{16})

Bit Byte	7	6	5	4	3	2	1	0
0	(msb) DVD STRUCTURE Data Length (0016_{16})							
1								(lsb)
2	Reserved							
3	Reserved							
4	(msb) ID_{media}							
:								
11								(lsb)
12	(msb) DVD-MAC(ID_{media})							
:								
21								(lsb)
22	Reserved							
23	Reserved							

This Command with this Format Code is used to carry out steps 2a and 2b of the protocol flow diagram shown in Section 6.2.

The **DVD STRUCTURE Data Length** field specifies the length in bytes of the following DVD STRUCTURE data that is available to be transferred to the Host. The **DVD STRUCTURE Data Length** value does not include the **DVD STRUCTURE Data Length** field itself. For a Format Code of 06_{16}, the value of this field is 0016_{16}.

Bytes 4 through 11 return the 64-bit ID_{media} value.

Bytes 12 through 21 return an 80-bit message authentication code (MAC), which is calculated using the Bus Key, and has the value:

DVD-MAC(ID_{media})

When the loaded disc is not CPRM compliant media (see the requirements in Section 6.3.1 for determining whether media is CPRM compliant), this command with Format = 06_{16} shall be terminated with CHECK CONDITION Status, 5/6F/01 COPY PROTECTION KEY EXCHANGE FAILURE - KEY NOT PRESENT.

When the DVD Logical Unit is not in the Bus Key state, this command with Format = 06_{16} shall be terminated with CHECK CONDITION Status, 5/6F/02 COPY PROTECTION KEY EXCHANGE FAILURE - KEY NOT ESTABLISHED.

6.3.3.2 MEDIA KEY BLOCK (Format 07_{16})

Table 6-9 – READ DVD STRUCTURE Data Format (With Format Field = 07_{16})

Bit Byte	7	6	5	4	3	2	1	0
0	(msb) DVD STRUCTURE Data Length (6002_{16})							
1								(lsb)
2	Reserved							
3	Total Packs							
4	(msb) MEDIA KEY BLOCK Pack Data							
:								
24,579								(lsb)

This Command with this Format Code is used to carry out steps 2a and 2b of the protocol flow diagrams shown in Section 6.1.

The **DVD STRUCTURE Data Length** field specifies the length in bytes of the following DVD STRUCTURE data that is available to be transferred to the Host. The **DVD STRUCTURE Data Length** value does not include the **DVD STRUCTURE Data Length** field itself.

The **Total Packs** field reports the total number of MKB Packs that are available for transfer to the host, which is the value of the Total MKB Packs Used field of the CPR_MAI table in the Control Data Area. The **Address** field in the command specifies which MKB Pack is read by the current command.

The **MEDIA KEY BLOCK Pack Data** field returns the Data field of the requested MKB Pack. For the first Pack only (command Address field = 00000000_{16}), the host must supply a valid AGID field, and the drive modifies the first 10 bytes of the Pack before returning it to the host. Specifically, the first 10 bytes of the MKB Descriptor are replaced with a message authentication code (MAC) of the original MKB Descriptor's MKB_Hash field, as shown in Table 6-10.

Table 6-10 – Modified MKB Descriptor, as Returned by Drive to Host

Bit Byte	7	6	5	4	3	2	1	0
0	DVD-MAC(MKB_Hash)							
:								
9								
10	000000000000_{16} (final part of Reserved field)							
:								
15								

The first 10 bytes contain an 80-bit message authentication code (MAC), which is calculated using a Bus Key and has the value:

DVD-MAC(MKB_Hash)

When the loaded disc is not CPRM compliant media (see the requirements in Section 6.3.1 for determining whether media is CPRM compliant), this command with Format = 07_{16} shall be terminated with CHECK CONDITION Status, 5/6F/01 COPY PROTECTION KEY EXCHANGE FAILURE – KEY NOT PRESENT.

When the DVD Logical Unit is not in the Bus Key state, this command with Format = 07_{16} shall be terminated with CHECK CONDITION Status, 5/6F/02 COPY PROTECTION KEY EXCHANGE FAILURE – KEY NOT ESTABLISHED.